

Department of the Interior
Report on the Implementation of the E-Government Act
Fiscal Year 2013

A. Enhanced Delivery of Information and Services to the Public - Sec. 101, 3602

Activity #1. Cloud Services: DOI awarded a \$10 billion Foundation Cloud Hosting Services contract in July 2013. This is a Multiple Award, Indefinite Delivery Indefinite Quantity (IDIQ) contract that was awarded to 10 different vendors and 7 service lines. Those service lines include virtual machine services, storage services, database hosting services, secure file transfer services, web hosting services, development and test environment hosting services, and SAP application hosting. The contract will streamline access to commercial cloud services in support of the Federal Data Center Consolidation Initiative (FDCCI), the Federal Cloud-First policy, the DOI Information Technology Transformation (ITT) Initiative, and emerging system owner demand for application and data hosting services. It will provide an attractive alternative to purchasing and maintaining hardware and software. The contract will help improve "speed to market" for developing and modernizing applications by providing our developers and system owners with access to computing and storage resources on demand. This will enable DOI to deliver services to the public taxpayer more efficiently, and with a lower capital expenditure. The contract provides the opportunity to shift from a capital intensive, asset-based perspective on delivering Infrastructure Services, to a service-based perspective. As a metered service, it is paid as an operating expense, after it is consumed, and based solely upon resources utilized, thus reducing the burden of providing large scale government operated infrastructure services. DOI expects this service model to be cost competitive, because it leverages the economies of scale, and maintains competition throughout the acquisition lifecycle. This contract leverages the Federal Risk and Authorization Management Program (FedRAMP), to evaluate and maintain security consistently across the government enterprise. The "Authorize Once, Use Many" approach of the FedRAMP processes and governance will simplify compliance activities, reduce the market barriers-to-entry, and unlock additional economies of scale for cloud service providers. The service lines available within the contract form the building blocks for defining future services, and were developed to meet the most urgent hosting needs for our internal customers. DOI has worked with the vendors on ensuring compliance with the FedRAMP processes and overall program. DOI has issued 1 internal task order to support the migration of the DOI Finance and Business Management System (FBMS) to a cloud environment, as well as one external (Federal Housing Finance Agency) task order. DOI has approximately 25 additional requirements that are currently in the queue moving through the cloud hosting technical evaluation and acquisition phases. DOI is also in the process of developing business processes to support the operation and management of the Foundation Cloud Hosting Contract to include the development of a StoreFront where all customers of the contract can learn about the options available, download forms/templates to be used in the process and points of contact information.

Activity #2. Unified Messaging: On August 1, 2012, DOI started its final phase of migrating to its contract for a cloud-based "Software as a Service" (SaaS) email and collaboration system. DOI met its goal in fiscal year (FY) 2013 to transition its email and collaboration services from thirteen disparate, on-premise systems to a highly integrated, innovative, creative, cost-effective, and evolving cloud-based environment that better serves its employees and the American people. In January 2013, the last group of DOI employees was migrated. The implementation of a suite of tools and capabilities now allows DOI to transform the way business is conducted with the American people, as well as manage and monitor service performance, quality, and delivery through clearly defined roles and business rules. DOI's Bureaus and Offices are now leveraging tools for increased collaborative consultation with partners and the public, improved information sharing and public comment, and more effective notice publication and issues representation among many other benefits. With all employees on one system, intra-department communication has been enhanced as new email, calendaring, and collaboration capabilities gain wider use. An employee survey indicated that 62% of survey participants rated the new system a "3" or higher on a scale from 1 to 5, with 5 being the most satisfied. The email component rated at 69% viewing it as "Very Easy" or "Easy" to use, giving the email application the overall highest ease of use rating among all of the features.

B. Capital Planning and Investment Control Procedures for IT - Sec. 101, 3602

In 2013, DOI Information Technology (IT) Capital Planning Investment Control (CPIC) team continued to mature its procedures through the establishment of a performance baseline management policy. The performance baseline management policy is intended to provide clear direction for how IT investment managers should be managing their baselines as DOI continues to work to mature its management of the IT portfolio baseline. The DOI CPIC team is also driving IT governance reform, consistent with OMB PortfolioStat, TechStat and M-11-29. During 2013, DOI continued implementation towards the target framework with the establishment of the Support Services Board, which has oversight responsibilities on a number of E-Gov investments.

In addition, the DOI CPIC team continued to integrate more closely with the Enterprise Architecture (EA) function in the development and maintenance of Line of Business (LOB) Segment Roadmaps. DOI established the LOB Segment Roadmap initiative to plan improvements in DOI's mission and support services Domains. The DOI Office of the Secretary Investment Review Board (OS IRB) surveyed the portfolio and recognized the need for a practical approach to meet business transformation objectives. The need was to develop a strategic implementation plan to improve the delivery and efficiency of business services and decisions that: align and prioritize investments and activities with business needs and funding; identify investments for consolidation, replacement or retirement; sequence investments and activities on a timeline for action; serve as a living document to guide the business on an ongoing basis; and identify areas for increased IT Cost Saving and/or efficiencies in spending.

A. Performance Integration - Sec. 202(b)

The DOI EA Program is involved in strategic planning and performance management at various levels of the organization. For example, the DOI EA Program has a direct involvement with the

OCIO Strategic Performance Framework, which is discussed in the Information Resources Management (IRM) Strategic Plan and is linked to the Department's Strategic Plan and Annual Performance Plan and Report (APP&R). DOI has established metrics and a measurement methodology for measuring the value of EA to DOI. The EA Program will perform the measurement process annually; update measures, re-baseline, identify appropriate targets and timelines, collect results, analyze results, and drive toward increased EA Program value. In addition, one of the key fundamental processes implemented by DOI's OCIO officials is managing IT organizational change. The staff's embracement of new initiatives was the identification of new performance metrics. The FY 2013 performance goals directly align with the Secretary's IT Transformation (ITT) Strategic Plan, as well as our Administration's priorities. DOI recognized the importance of establishing targets and monitoring actual performance to effectively achieve ITT goals. FY 2013 requirements were heightened in our Information Resource Management (IRM) Organizational Assessment (OA) that was used to identify Bureau/Office IRM quarterly (Q) ratings.

The following OA components have been established to support DOI's ITT Strategic Plan which is accessible via: <http://www.doi.gov/ocio/index.cfm>.

B. Accessibility - Sec. 202(c) and (d)

Public Facing Agency URL(s)	Brief Explanation (if necessary)
http://www.doi.gov/ocio/information_management/section-508.cfm	DOI Section 508 website

C. Government-Public Collaboration - Sec. 202(e)

The U.S. Geological Survey (USGS) is incorporating data obtained from volunteers to update information about the location and names of common buildings such as police stations, fire stations, schools, and hospitals. This information becomes part of The National Map (<http://nationalmap.gov>) once it has undergone appropriate quality assurance. The National Map is a set of national databases that contain basic map information for the United States. The USGS typically maintains information in The National Map through partnerships with other governmental agencies and contracts with private sector firms. While the USGS has had a volunteer program in the past to maintain map information, technological advancements have made it much more feasible for the public to provide accurate locational information and for the USGS to incorporate this information into The National Map. As of November 1, 2013, over 1,000 volunteers have joined the project and over 18,000 edits have been made to the data in The National Map. The USGS is working with national volunteer organizations, including 4-H and the GISCorps, to recruit additional volunteers. A set of virtual badges have also been established to reward volunteers for providing a specified number of edits. More specific information about the volunteer program can be found at: <http://nationalmap.gov/TheNationalMapCorps/index.html>.

D. Credentialing - Sec. 203

In early FY 2013, DOI completed its Department-wide move to a cloud-based email system, which relies extensively on the authentication, authorization, and federation services components DOI deployed in FY 2012, as a DOI-managed, federally controlled external directory service. This external directory service continues to provide both authentication and authorization services to external partners and collaborators who use the Department's on-premise collaboration systems. Continuing its expansion of cloud hosting and cloud services, in late FY 2013, DOI successfully awarded a major Cloud Hosting contract that it views as foundational to establish the core capability DOI will use to accept externally issued credentials. As more and more of the agency's web systems move to the cloud, DOI has determined that it can be more effective and less expensive to implement a single cloud-based authentication system to negotiate externally issued credentials and authentication claims, than to build this function into its existing, on-premise SAML Service Provider infrastructure. In FY 2014, DOI will explore the possibility of obtaining these services through its Foundational Cloud Hosting contract in order to meet the goals of the Chief Information Officer (CIO) Memorandum, "Requirements for Accepting Externally-Issued Credentials."

DOI's FY 2013 activities in support of the Memorandum were focused primarily on:

As web systems inventory and prioritization resulting from systems analysis draws to a close, DOI will select Trust Framework Providers. Services available through DOI's Foundational Cloud Hosting contract will provide the basis for the framework the Department will implement in FY 2014 to enable Level 1 and Level 2 websites, where appropriate, with authentication using externally issued credentials. DOI expects full implementation within the next year, per the Memorandum.

E. USA.gov activities - Sec. 204 and Sec. 207(f)

Public Facing URL(s)	Brief Explanation (if necessary)
http://www.usa.gov/directory/federal/department-of-the-interior.shtml	DOI USA.gov activities

F. eRulemaking - Sec. 206

The eRulemaking Program has simplified public participation in DOI's rulemaking process by making regulatory information more available and accessible on Regulations.gov. This website increases opportunities for public involvement in DOI's rulemaking process by making it easier to submit comments on proposed rules published by the Department.

In FY 2013, DOI posted 106 rules and 207 proposed rules, 100 Federal Register notices, and 63,539 public submissions in Regulations.gov. Overall, DOI provides public access to 66,383 documents in Regulations.gov.

The eRulemaking Program offers streamlined internal rulemaking business processes with agency access to the Federal Document Management System (FDDMS) –i.e., via FDMS.gov.

DOI had 143 staff using FDMS.gov in FY 2013, and created --- regulatory dockets in FDMS for new regulatory actions published in FY 2013. DOI has received 63,539 public comments via Regulations.gov that are directly stored in FDMS.

G. National Archives Records Administration (NARA) Recordkeeping - Sec. 207(e)

DOI established the electronic eMail Enterprise Records and Document Management System (eERDMS) program to move the agency toward an integrated electronic enterprise recordkeeping system that provides support for messaging, records management, content management, case management, and early case assessment review. The eERDMS program consists of the following five systems: Enterprise Forms System (EFS), Enterprise eArchive System (EES), Enterprise Dashboard System (EDS), Enterprise Content System (ECS), and Enterprise Fax System (EXS). These systems provide a Department-wide solution to increase cost savings and improve greater efficiencies for managing records in a Department of Defense (DoD) 5015.2 compliant records management environment.

DOI has a total of 425 electronic systems as of FY 2013, of which 345 have been scheduled. There were 80 electronic systems submitted to NARA for approval, of which 64 were approved and 16 are pending approval. The NARA-approved records schedules and description of the records systems are available at http://www.doi.gov/ocio/information_management/information_dissemination.cfm.

H. Freedom of Information Act (FOIA) - Sec. 207(f)(A)(ii)

Public Facing Agency URL(s)	Brief Explanation (if necessary)
Primary FOIA website: http://www.doi.gov/foia/index.cfm	DOI Freedom of Information website

I. Information Resources Management (IRM) Strategic Plan - Sec. 207(f)(A)(iv)

Public Facing Agency URL(s)	Brief Explanation (if necessary)
http://www.doi.gov/ocio/index.cfm	DOI IT Transformation Strategic Plan (dated June 2011) - For FY 2010 - FY 2015, and May 2013 Draft

J. Public Access to Electronic Information - Sec. 207(f)(B)

Public Facing Agency URL(s)	Brief Explanation (if necessary)
http://www.doi.gov/open/index.cfm	DOI Open Government Initiative website
http://www.doi.gov/open/upload/Customer-Service-	DOI Customer Service Plan

Public Facing Agency URL(s)	Brief Explanation (if necessary)
Plan-DOI-10-23-2011.pdf	
http://www.doi.gov/digitalstrategy/index.cfm	Digital Government Strategy Report website
http://www.doi.gov/notices_soc.cfm	Final determinations, priorities, and schedules for each E-Gov initiative:
http://www.doi.gov/archive/ocio/egov/products.html	Information dissemination product catalogs, directories, inventories, and any other management tools used to improve the dissemination of and access to information by the public

K. Research and Development (R&D) - Sec. 207(g)

Public Facing Agency URL(s)	Brief Explanation (if necessary)
http://www.doi.gov/archive/ocio/egov/research.html	Public websites disseminating research and development (R&D) information

L. Privacy Policy and Privacy Impact Assessments - Sec. 208(b)

DOI is committed to protecting individual privacy and promoting a culture of privacy compliance. To balance the potential risk to privacy against the need to fulfill DOI's mission, DOI implemented policy and controls that are aligned with OMB policies and National Institute of Standards and Technology (NIST) guidance and standards for the protection of sensitive information. These policies and controls ensure that agency personally identifiable information (PII) is only accessed by authorized personnel and increase accountability for individuals with responsibilities related to safeguarding sensitive information.

DOI privacy policy is focused on ensuring appropriate safeguards to protect PII and the confidentiality, integrity and availability of information privacy. DOI has implemented a combination of technical, administrative and physical controls to safeguard personal information from inappropriate or unauthorized access, use, or disclosure in alignment with OMB policy and NIST guidance. DOI uses operational controls and privacy enhancing technologies, such as data loss prevention software, encryption, firewalls, authorized use system access controls, and system audit logs; and has effectively reduced the risk of compromise of sensitive PII in agency communications by implementing a Data Loss Prevention (DLP) solution, that monitors network communications and prevents sensitive PII from leaving the network.

In addition to these technical controls, DOI utilizes administrative policies and procedures, as well as privacy training, to further safeguard information privacy and control access to information systems and information assets. The DOI PIA Guide includes a privacy impact assessment (PIA) template and guidance on conducting PIAs in accordance with the E-

Government Act of 2002 and OMB M-03-22. DOI conducts PIAs on all information systems, third-party websites and social media applications to ensure privacy implications are addressed when planning, developing, implementing, and operating information systems that maintain information on individuals. DOI privacy office personnel collaborate with system owners and IT security to assess new or proposed programs, systems or applications for privacy risks, and recommend methods to protect individual privacy.

As part of the DOI PIA compliance review cycle, PIAs are updated whenever changes occur to the information system or process, or every three years. This ensures privacy implications are addressed during the system life cycle, and demonstrates that the agency has evaluated privacy risks and incorporated protections commensurate with those risks to safeguard the privacy of personal information. The DOI PIA Guide also provides guidance for completing PIAs to ensure that PII is only collected as authorized, that system of records notice requirements are met, and that appropriate security controls are implemented to protect and manage access to PII within DOI information systems.

DOI maintains an inventory of PIAs within the Cyber Security Assessment and Management (CSAM) system, the Department's official information system repository. This centralized repository allows the DOI Privacy Office to conduct regular reviews of bureau and office PIA inventories, identify and correct PIA deficiencies, as well as assess compliance with privacy laws, policies and standards. This provides for an efficient PIA review process, and facilitates management of PIAs for new and existing information systems.

L2. Privacy Policy and Privacy Impact Assessment Links - Sec. 208(b)

Public Facing Agency URL(s)	Brief Explanation (if necessary)
http://www.doi.gov/privacy.cfm	DOI Privacy Policy
http://www.doi.gov/ocio/information_assurance/privacy/ppia.cfm	DOI Privacy Impact Assessments

N. Agency IT Training Programs - Sec. 209(b)(2)

In FY 2013, as follow-on to the spring 2012, DOI IT skills assessment of 1,000+ IT skills and 14 behavioral and business competencies, DOI conducted a comprehensive Current State IT workforce analysis that identified the major duties of each IT position throughout all DOI Bureaus and Offices. This analysis aligned major IT duties to Infrastructure IT or Mission Program IT. In addition, the Infrastructure IT duties were further assigned to 6 major IT Service Domains along with their service categories and sub-categories. The Infrastructure IT Service Domains included (1) End User Services and Support/Wireless Control Services, (2) Help Desk/Enterprise Service Desk, (3) Hosting, (4) Information Assurance and Computer Network Defense, (5) Telecommunications, and (6) IT Policy, Planning and Compliance/IT Management. This detailed workforce duty analysis provided DOI IT leadership with a comprehensive view of the IT work being performed across the Department. The data has been instrumental in

workforce planning required by the Bureaus and Offices to support IT Transformation and will continue to be used throughout DOI's IT Transformation.

The next step in DOI's IT workforce development is to map the major duties in DOI's future state organization to the current state skills assessments so that IT managers can identify more targeted training and development opportunities for their employees. This gap analysis is intended to ensure that development is clearly aligned to the direction the Department is taking with IT Transformation. To date, they have done this mapping for 20 IT positions that were recently revised to meet the immediate and future IT needs of DOI in the areas of Unified Messaging, Hosting, Cloud Management and Customer Relationship Management. Throughout FY 2014 and into FY 2015, DOI will continue to define additional operational details for the IT Transformation future state and identify the related competencies needed to achieve that future state. As each segment of the IT organization is transformed, DOI will continue to compare the IT workforce future state requirements to the IT workforce skills and competency assessment data to determine gaps. To close the gaps, DOI will develop a comprehensive, DOI-wide IT workforce training and development plan to ensure the successful execution of the IT future state. DOI also continues to focus on the importance of having qualified, skilled IT project and program managers. In collaboration with DOI University, DOI offers a Federal Acquisition Certification for Program and Project Managers (FAC-P/PM). Individual classes or the full curriculum resulting in certifications are available. On-line project management classes are available to DOI employees through a Skillsoft license, which can be purchased for \$40/year.

In addition, the DOI Privacy Training Program includes a mandatory Privacy Act course that is delivered as part of the Federal Information System Security Awareness (FISSA) training that must be completed by all new employees and contractors, and annually thereafter. Specialized training courses and individual or group training are provided to increase privacy awareness and ensure compliance with Federal privacy laws and policies. In FY 2013, DOI developed two computer-based privacy courses, Privacy for HR/EEO Professionals and Privacy and Civil Liberties in the Information Sharing Environment, to provide targeted, role-based training to employees with privacy responsibilities. These courses provide guidance on roles, responsibilities and compliance requirements, and are available to all agency employees on DOI Learn, DOI's Department-wide learning management system.

P. Geospatial - Sec. 216

Introduction

As the home of the Executive Secretariat for the Federal Geographic Data Committee (FGDC), and in our relatively new role as the Managing Partner for the OMB Shared Services initiative, the Geospatial Platform, the DOI plays an important role in helping to facilitate the government's efforts in these areas. In FY 2013, several activities and accomplishments were particularly noteworthy, including our ongoing efforts to develop the Geospatial Platform; our work towards developing a new Strategic Plan for advancement of the National Spatial Data Infrastructure; and continuation of our ongoing efforts to develop, adopt and promote geospatial technology standards for the federal government.

Geospatial Platform

The federal geospatial community's collaborative efforts through the Geospatial Line of Business (LoB) successfully transitioned to the OMB Shared Services initiative "Geospatial Platform" whose activities focused on the implementation of Geoplatform.gov as a mechanism for developing and delivering geospatial shared services across government. The Geospatial Platform activity demonstrates advancement in our collaborative effort to support geospatial activities across Federal, State, local and Tribal agencies and helps to improve the efficiency of government by making trusted geospatial data, services and applications more accessible, reliable, and less expensive to acquire through enhanced data-sharing and more effective management of resources via shared infrastructure and enterprise solutions. Version 2.0 of Geoplatform.gov was released in July of 2013 with new features and capabilities being released on a regular basis. Major release features include:

National Spatial Data Infrastructure (NSDI) Strategic Plan

DOI and its partners from the FGDC agencies led an effort to develop a new Strategic Plan for the National Spatial Data Infrastructure (NSDI) through extensive outreach and collaboration with Federal agencies, external partners, and the National Geospatial Advisory Committee. The plan will describe a shared national vision for the NSDI and outline the actions the Federal government will take to contribute to this vision. One of the FGDC's responsibilities under OMB Circular A-16 is to "prepare and maintain a strategic plan for the development and implementation of the NSDI." Executive Order 12906 describes the NSDI as "the technology, policies, standards, and human resources necessary to acquire, process, store, distribute, and improve utilization of geospatial data." A new NSDI plan is important and timely because the FGDC has engaged in a series of strategic initiatives over the past several years, including the Geospatial Line of Business and Geospatial Platform, but the current NSDI strategic plan has not been revised for a number of years. Secondly, geospatial technologies, industries, and applications have evolved over the past several years, and our strategies need to be modernized to align with and leverage these changes. In addition, a recent report by the Government Accountability Office (GAO), "GAO-13-94", reaffirmed the importance of improving coordination and reducing potential duplication and recommended the development of an updated NSDI strategy.

Geospatial Data and Technology Standards

In FY 2013, the FGDC formally endorsed 5 geospatial technology standards to be used by all federal agencies that leverage geospatial information. Throughout FY 2013, the FGDC continued its strong support of external standards activities, consistent with the directives of OMB Circular A-119 on Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities. The FGDC and member agencies continued to participate in the InterNational Committee on Information Technology Standards Technical Committee L1 (INCITS L1), Geographic Information Systems, which is the means by which segments of the geospatial community participate in American National Standards Institute (ANSI) and International Organization for Standardization (ISO) geospatial standardization

activities. INCITS L1 serves as the U.S. Technical Advisory Group to ISO Technical Committee 211, Geographic information/Geomatics.

The FGDC also continues to be an active participant in the Open Geospatial Consortium (OGC), an international industry consortium of over 460 companies, government agencies and universities participating in a consensus process to develop publicly available interface standards. FGDC Community members participate in the OGC working groups and Interoperability programs, bringing the community needs into the OGC process.